Attachment A

The State of Montana's Acceptable Internet/E-Mail Use Policy

Operations & Technology Division
Internet, Intranet, & E-Mail Acceptable Use Policy

Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare.

Scope: This policy applies to all Department employees and state contractors using DPHHS computers.

Policy Statement: Internet, Intranet and E-Mail access provided by the department is intended for department business use, but limited access for personal use is allowed. The department encourages the use of the Internet, Intranet and E-Mail, because they make communication and research more efficient and effective. Use of the department time, facilities, equipment or supplies for an employee's private business, either for profit or non-profit, is statutorily prohibited and is a misdemeanor crime, Section 2-2-121, MCA. Every employee and contractor has a responsibility to maintain and enhance the Department's image and to use the Internet, Intranet and E-Mail in a productive manner. To ensure that all employees and contractors are responsible, the following guidelines have been established for use of the Internet, Intranet and E-Mail.

Acceptable Use: Internet, Intranet and E-Mail use is intended for state business purposes but employees may use these services for personal use with certain restrictions. Personal use may be permitted at the discretion of the employee's supervisor. Personal use of the Internet is not considered part of an employee's paid work time. The supervisor determines at what times during the day the Internet, Intranet and E-Mail may be accessed for personal use by their employees. The supervisor may prohibit employees from using the Internet at any time. The Department of Administration manages Internet filtering (blocking) of individual websites or classes of websites. Requests for exceptions to any filtered site should be directed to the DPHHS Security Manager, who can also provide a list of currently filtered sites.

Misuse of Computer Resources:

The department-provided Internet, Intranet and E-Mail access may not be used **at any time** for:

- Transmitting, retrieving or storing any communication of a discriminatory or harassing nature, or materials that are offensive, obscene or x-rated. Examples of offensive, obscene or x-rated materials include but are not limited to: items, either pictures, movies or text, which describe or depict nudity, sexual activity, sexual offenses against individuals or other situations involving a sex act, or which describe or depict other bodily functions or situations which are inappropriate in business setting.
- Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered child pornography.
- Any purpose which is illegal, or is against state or department policy.
- For-profit and non-profit business activities including activities for service organizations not related to the job.
- Excessive use for private, recreational or personal activities.
- Gambling.
- Raising funds for political candidates or issues.
- Promoting political candidates in any way.

- Promoting personal political issues.
- Gathering information for furtherance of a crime.
- Circulating chain letters.
  Using personal E-Mail accounts, such as Hotmail, Yahoo, AOL etc without permission from the DPHHS Security Officer.
- Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening or discriminatory materials.
- Downloading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
- Use of computers and UserIDs for which there is no authorization, or use of UserIDs for purposes outside of those for which they have been issued.
- Attempting to modify, install or remove computer equipment, software, or peripherals without proper authorization. ***This includes installing any non-work related software on State-owned equipment.***
- Accessing computers, computer software, computer data information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State. (This means, if you use the networks to which the State has access or the computers at other sites connected to those networks for which you do not have authorization, the Department will consider this matter an abuse of your computing privileges, and violation of this policy.)
- Circumventing or attempting to circumvent logon procedures, and security regulations, or exceeding the system's capacity limits by downloading excessive materials.
- The use of computing facilities, UserIDs, or computer data for purposes other than those for which they are intended or authorized.
- Breaking into another user's E-Mailbox, or unauthorized personnel reading someone else's E-Mail without permission.
- Sending fraudulent electronic transmissions, including but not limited to statements intended to mislead the receiver and are known to be untrue, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Taking advantage of another user's naiveté or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorization to access.
- Physically interfering with other users' access to the State's computing facilities.
- Encroaching on or disrupting others' use of the State's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); excessive use of using memory, bandwidth and disk space resources; interfering with connectivity to the network; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a State computer; damaging or vandalizing State computing facilities, equipment, software, or computer files).
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission. This does not prohibit supervisors having access to their employees' computers.

Generating, Receiving and Maintaining Electronic Records: All messages created, sent or retrieved over the state's system are the property of the State of Montana. Employees should not have expectations of privacy for any messages. In drafting or sending E-Mail messages, employees should not include anything that would not be appropriate for dissemination to the public. E-Mail communication must reflect professional and respectful business correspondence. Electronic communications will be monitored for performance, trouble-shooting purposes, and detection of abuse. In addition, employees should use their best judgment in sending messages that contain information required by law to be confidential.

Information Technology Services Division staff, during the course of their analysis, will monitor and report any access to a site or class of sites that does not appear to be work related and that is of sufficient volume that may be a potential capacity issue to ITSD management.

Communication sent or received by the E-Mail system may be considered "documents" under Article II, Section 9 of the Montana Constitution or public records under section 2-6-101, MCA, and may be subject to public disclosure. Therefore, care should be taken in generating and maintaining these records. Release of information to a member of the public regarding an employee's use of the Internet or E-Mail, or requests from law enforcement for records not otherwise available to the public involving an employee's Internet or E-Mail records can only be approved by the appropriate Division Administrator. This does not preclude ITSD or any other agency from contacting law enforcement as part of an investigation initiated by the agency. Agency legal counsel should be consulted whenever a court order is served or an investigation involves contact with law enforcement.

Employees should consider the following to better manage E-Mail activities:

- Employees should delete items from their in-tray and out-tray when they are no longer needed. If a mail item needs to be retained it should be moved to an archive folder, a disk, or be printed. Items placed in an employee's archive should be evaluated after six months to determine if they should be retained. Employees can contact the DPHHS Records Manager with any questions on retention schedules.
- Unsolicited mail should be deleted immediately. If the problem persists, contact the DPHHS Security Officer.
- Employees should check their E-Mail with a frequency appropriate to their jobs and as directed by the supervisor. Employees who will be absent for more than one day should utilize the "out of office" feature, or make arrangements for a supervisor or co-worker to check for messages that need attention.
- It is possible to receive a virus when receiving E-Mail, and some viruses are embedded in attachments. If you receive a suspicious E-Mail, do not open it, but instead contact the DPHHS Technology Services Center at 444-9500.
- Some computer features increase E-Mail traffic, and employees should strive to keep message and attachment sizes as small as possible. Avoid the use of graphics in auto-signatures or other parts of the message or attachments. Use of stationary should be avoided, as well as moving graphics and/or audio objects as they consume more disk space, network bandwidth, and detract from the message content.
- Users must log off the network at the end of each day and power off their workstations. Department resources should be logged off when not is use.
- Users leaving their computers unattended for more than 15 minutes should consider logging off the network.

Reporting Violations: Users will cooperate with DPHHS Management concerning requests for information regarding computing activities; follow Department and State procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow Department procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the Acceptable Use policies of any non-state networks accessed. Contact the DPHHS Technology Services office at 444-9500 for information on the policies and guidelines. Copies are attached.

Users will report unacceptable use and other security violations to their immediate supervisor, the DPHHS Security Officer or the Human Resources Office.

Each employee is responsible for the content of all text, audio or images that they place or send over Internet, Intranet or E-Mail. No E-Mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. All messages communicated on the Internet, Intranet or E-Mail system should contain the employee's name.

Copyright Issues: Department employees must honor copyright laws regarding protected commercial software or intellectual property. Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement. Department employees shall not make copies of software or literature in violation of copyright laws without the full legal right to do so. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyright material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. Copyrighted agency information used on web sites must be clearly labeled as such.

Training: Employees are required to attend E-Mail training prior to using the State of Montana E-Mail system. Training may include formal classes or on the job instruction. Employees should have the opportunity to attend training on the use of the Internet, but it is not required.

Internet Use Agreement: All Department employees having access to the Internet and E-Mail must acknowledge that all network activity is the property of the State and should not consider any Internet activity to be private. An electronic form of the Internet Use Agreement is accessible (Public Folder and DPHHS Website) and is meant to ensure that every employee with Internet and E-Mail access is familiar with the Department policy. Each user is required to read and understand the policy and acknowledge by completing the form.

Security: The department reserves the right to access and monitor any messages or files. Employees should not assume that electronic communications are private and should transmit highly confidential or personal information another way rather than by electronic means. Users are responsible for controlling the access to their computers, properly logging on and off the network, and not using another employee's UserID.

Contact the DPHHS Technology Services Center at 444-9500 with questions concerning this policy. You may also call this number for more information on the Information Security and Database Access procedures.

Violations of this policy may result in disciplinary action up to and including termination of employment with the Department.